Ping Identity Submission to the Consumer Data Right in Energy Consultation Process

20 March 2019

Summary

Ping Identity ("Ping") is pleased to submit this response to the consultation process for a Consumer Data Right in Energy, announced by the ACCC on 25 February 2019.

As described in our submission to the Australian Treasury Open Banking review in 2018, we believe the Consumer Data Right will set the course for secure digital interaction between service providers and application developers. A fundamental building block for Australia's digital future is enabling secure, consent-driven open data services across all industries.

Our expertise lies in the standards and technology necessary to successfully implement identity-based services at internet scale.

In this response, we draw on our experience in developing and implementing industry open standards like SAML 2.0, OAuth 2.0 and OpenID Connect 1.0; the latter two being the security foundation of modern internet security regimes, like Open Banking.

Mark Perry, Ping's Chief Technology Officer in Asia Pacific, is a member of the Australian CDR Advisory Committee, and has been vocal in supporting open standards for banking and other initiatives concerned with data sharing and open APIs. We also note our long history in the identity security industry's standards bodies (the IETF, the OpenID Foundation, the W3C for example), helping to author the protocols described in this submission and used by companies worldwide to secure their applications and services.

Ping's recommendation is that Model 3 is the best option of those offered, based on our experience with CDR/Open Banking in Australia and overseas, and other identity security regimes around the world. Model 2 would be the next best option. Model 1 has significant issues, described in more detail below, therefore we cannot endorse it for use in this regime.

Discussion regarding ACCC Questions

Question 1 — Are there any other assessment criteria or relevant considerations which the ACCC should use to determine a preferred model for consumers to access their energy data under the CDR?

Above all, the rights of the consumer should take precedence in the creation of the Energy CDR. In particular, consumer data should be treated as sensitive and deserving of IT industry-standard controls and processes. While energy industry data might not appear to be sensitive on the surface, data that can be attributed to and connected to individuals can be used for nefarious purposes. Previous breaches of consumer data have lead to significant loss of reputation and revenue for organisations, and have caused company executives to lose their jobs.

Ping believes that all consumer data should be afforded the same level of protection. Data should be encrypted at rest as well as in transit. Multi-factor authentication for accessing and transacting with consumer data should be mandatory. Well supported and tested Industry standards for credentials, authentication and authorisation should be used for this data sharing regime. This should have the additional benefit of reducing the cost of implementation, integration and on-going maintenance for all participants.

Consumers must be in control of their data sharing options, via informed consent. Significant work has been done on end user consent models, and this should be reused where possible.

The creation of a single database of consumer data should be avoided to limit the possibility of an all-encompassing data breach, which would damage the reputation of the regime.

Question 2 — Having regard to the assessment criteria, what are the advantages and disadvantages of each of the models?

We believe that the three models presented by the ACCC have different advantages and disadvantages. Based on our experience with Open Banking in Australia and overseas, and other identity security regimes around the world, in our opinion a fully decentralised model is best placed to serve the needs of the consumer and the industry in the long term.

We recommend the use of Model 3, as described by the ACCC in their Consultation paper of February 2019, with the addition of a central directory that only stores a list of certified participants (Data Holders and Data Recipients), and provides the security material (digital certificates and software statements) to remove the need for point-to-point connections between the two sets of participants.

If Data Holders are not in a position to implement the full set of API and security requirements to integrate with a Model 3 regime, Model 2 would be the next best option in our opinion.

Model 1, the AEMO centralised model, would potentially be easiest and cheapest for the industry as a whole, but would be an attractive “honeypot” (a central source of consumer data and end user credentials) for would-be attackers. With this model, a breach of the system would raise significant concern for consumers and damage the reputation of the entire regime.

This model would have the least impact on Energy Participants, as they would only need to transform their data into a standard format for transmission to AEMO.

Energy Participants would not need to manage end user access, including credentials.

However, this is also potentially a point of contention for those organisations who may already have an online relationship but wish to create a closer relationship with their customers through the CDR. Having their customers authenticate via AEMO, using credentials supplied by AEMO, may not be an acceptable model for those Energy Participants.

For consumers, this may also be potentially confusing and annoying. For example, if I already have an Origin Energy account, why can't I use that for performing Energy CDR transactions? Why should I have to create an account with AEMO, with whom I have no direct commercial relationship?

For these reasons, Ping finds this model to be the least desirable of the three offered.

Model 2, the AEMO gateway model, is an improvement on Model 1, as it limits the data being held centrally. It also minimises the infrastructure requirements for Data Holders compared to Model 3. This model will succeed or fail based on the scalability and resilience of the AEMO gateway.

A direct connection to the data holder for authentication makes this a more desirable model for consumers and some data holders.

From the description of this model, it is currently not clear who will generate the token to be used for API access. Authentication happens at the data holder, which will need to supply a token to the AEMO gateway as a way of authorising the data recipient to access the APIs on behalf of the consumer. As AEMO is the gateway for API access, this gateway will need to validate tokens from multiple data holders; a less-than desirable model, although still technically feasible.

It is for this reason that Ping cannot support this model as the best of those offered.

Model 3, the economy-wide CDR model, is the most favourable in terms of security and, potentially, resilience. This fully decentralised model (with the addition of a directory of certified participants) would be Ping's recommendation.

Consumers will authenticate against their energy retailer(s) of choice, who will in turn supply tokens for accessing the APIs, which they host and manage. This is the most technically feasible mode of the three, and is the most supported by the industry.

One issue with this model could be the existing level of maturity of energy data holders in Australia, in terms of their IT security and API infrastructures. Without knowing the full details of each data holder, and the desired timeframe for implementation of the Energy CDR, it is not possible for Ping to ascertain what the impact of this model would have on those organisations.

Question 3 — What are the likely implementation/compliance costs for market participants (including accredited data recipients) under each of the models, including costs associated with IT system changes or data storage?

Ping cannot estimate the actual costs of implementation and compliance for the energy sector. However, we note that commercial off the shelf products exist to implement open API and standards-based data sharing, requiring little if any custom coding, reducing costs for participants.

In line with our recommendations about data security previously, we would expect there to be an impact on data holders to secure data at rest if Models 2 or 3 are implemented.

Models 2 and 3 also require modern API security technology, that supports OpenID Connect, to work with today's API gateway technology. As this standard is well supported by industry, there are a significant number of technology options for this standard.

Question 4 — What additional requirements should the ACCC consider including in the CDR rules for the energy sector if the gateway model is adopted?

If the gateway model is adopted, the ACCC, should work hard to resist any desire to store user data in the gateway itself, to help prevent the opportunity for whole-of-regime data breaches.

Question 5 — What emerging technologies do stakeholders believe will have an impact on the energy sector with respect to the CDR?

Existing open standards security technologies, like OpenID Connect, have been successfully used in Open Banking programmes and should definitely be reused for the Energy CDR. We would advise against straying too far from accepted and tested standards for security, as the potential for security issues is minimised where tried and tested options are used.

Question 6 — What are the cost differences to participants of providing data once a day (to an AEMO repository) or on demand?

Ping Identity has no firm opinion on this question.

Question 7 — What is the competitive impact, if any, of accessing data through AEMO rather than through a retailer?

As stated in our previous comments, consumers would not authenticate using their local Energy Participant credentials in Model 1. This could potentially be a commercial disadvantage for some Energy Participants and is not supported as a model by Ping Identity for this reason, amongst others.

Question 8 — Are there any other issues that stakeholders wish to raise?

Ping wishes to reiterate that building on the open standards and process started by the ACCC and Data 61 for the CDR is essential for a consistent approach to Open APIs and consent-driven data sharing.

Conclusion

Ping Identity is excited for the future of the Consumer Data Right in Australia and will contribute our experience and know-how to help this important initiative move forward.

We believe this work will ultimately benefit consumers as well as established and emerging companies, while safeguarding privacy and security.

We look forward to collaborating on this effort with the government, fellow IT industry participants, third parties interested in consumer rights and privacy, and the energy industry, to build a solid, secure and consent-driven framework for Australia's digital future.